TITLE OF THE INVENTION

METHOD FOR ENCRYPTING AND DECRYPTING CONTENTS DATA DISTRIBUTED THROUGH NETWORK, AND SYSTEM AND USER TERMINAL USING THAT METHOD

BACKGROUND OF THE INVENTION

1. Field of the Invention

本発明は、コンテンツデータを、ネットワークを介してサーバから配信する際の暗号化・復号化に関する。

2. Description of the Related Art

ネットワークを介して配信されるデータ提供サービスにアクセスしてログインする方法として、最も普及しているのはユーザIDとパスワードを入力する方法である。

しかしながら、ユーザIDもパスワードも共にデータとしてネットワークを介して送受信される。もし、第三者が何らかの方法でこのユーザIDとパスワードをネットワークから取得し、正規のユーザになりすましてログインした場合、サーバ側では正規のユーザかどうかの判別ができず、不正なアクセスが行われることになる。

そこで、ログインに係る安全性を高めるために、パソコンに装備されるインタフェースポート（パラレル、シリアル、ＵＳＢ等）に接続するＨ／Ｗ（ＨＡＲＤＷＡＲＥ）キーを使用する方法が考えられている。このＨ／Ｗキーは複製が困難であり、正規のユーザ以外の第三者が簡単に取得することはできない。Ｈ／Ｗキーは、例えば会社の社員が社内のデータベースにアクセスするエクストラネットや、ショッピングやバンキングなどの会員限定サービス等で使用されている。

これらにおいて、Ｈ／Ｗキーの役割は、容易かつ信頼性の高いユーザの特定にある。すなわち、このＨ／Ｗキーを用いた認証システムは、サーバ上のプログラムに対して、コマンドの発行やデータを入力する権限を守ることが主目的である。そのため、ネットワークを介してサーバから配信されるコンテンツデータ自体

は保護されない。つまり、オンライン状態でサーバから配信された画面データをユーザ端末で保存し、オフライン状態になってからユーザ端末で再度見ることも可能である。

従って、著作権の存在する電子化されたコンテンツデータの配信にあたっては、その不正な再生、複写等を防止して、コンテンツデータの著作権を保護する必要があり、近年コンテンツデータの保護機能を有したコンテンツデータ再生装置が使用されるようになった。

以下、図５を参照して、コンテンツデータ再生装置について説明する。

図５は前記コンテンツデータ再生装置の機能ブロックの構成を示す。図５において、１０１は、コンテンツデータ再生装置である。１０２は、暗号化されたコンテンツデータを入力する入力部である。１０３は、暗号化されたコンテンツデータを復号化するための共通キーが格納される共通キー蓄積部である。１０４は、暗号化されたコンテンツデータを、共通キー蓄積部１０３に格納された共通キーを用いて復号化する復号部である。１０５は、コンテンツデータを人間の視聴覚もしくは触覚等で感知できる状態に再生する再生部である。

以上のように構成されたコンテンツデータ再生装置１０１について、以下にてその動作を説明する。

まず、通信路等を介して外部から暗号化されたコンテンツデータが入力部１０２に入力され、復号部１０４に送られる。共通キー蓄積部１０３にあらかじめ格納されている共通キーが読み出され、復号部１０４に送られる。復号部１０４では、共通キー蓄積部１０３から提供された共通キーを用いて、暗号化されたコンテンツデータの不正改ざんのチェック、及び前記暗号化されたコンテンツデータの復号化を行う。復号化されたコンテンツデータは、再生部１０５に送られる。再生部１０５において、人間の視聴覚もしくは触覚等で感知できる状態に再生され、出力される。

しかしながら、上記の構成では、暗号化されたコンテンツデータを復号化するための共通キーは同じ値が固定的に使用され、コンテンツデータ再生装置内に常時保存されている。従って、ハッカー等が、外部から通信路を介してコンテンツデータ再生装置１０１の中に不正に進入して、共通キーと暗号化されたコンテン

ツデータを取得する可能性がある。このように共通キーとコンテンツデータが不正に取得された場合は、他の同種の装置を用いて再生できてしまい、コンテンツデータの著作権が侵害されてしまう。

従って、暗号化されたコンテンツデータを複合化するためのキーの不正取得や、コンテンツデータの不正な再生を防止することができるコンテンツデータの暗号化・復号化方法の必要性がある。

BRIEF SUMMARY OF THE INVENTION

According to an aspect of the present invention, 配信されるコンテンツデータのコンテンツ情報から、第１キーをサーバにて生成する。可変パラメータと、Ｈ／ＷキーＩＤと、第１キーとから、第２キーをサーバにて生成し、生成された第２キーをユーザ端末に送信する。可変パラメータと、Ｈ／ＷキーＩＤと、第２キーとから、第１キーをユーザ端末にて復号化する。配信されるコンテンツデータを、第１キーで、サーバにて暗号化し、暗号化されたコンテンツデータをユーザ端末に送信する。暗号化されたコンテンツデータを、復号化された第１キーで、ユーザ端末にて復号化する。

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings, which are incorporated in and comprise a part of the specification, illustrate presently embodiments of the invention, and together with the general description given above and detailed description of the embodiments given below, serve to explain the principles of the invention.

図１は、本発明の第１の実施の形態に係る暗号化・復号化システムを説明するブロック図である。

図２は、同実施の形態におけるユーザ端末の構成図である。

図３は、同実施の形態における暗号化・復号化の動作を示すフローチャートである。

図４は、別の実施の形態である暗号化・復号化の動作を示すフローチャートである。

図５は、従来のコンテンツデータ再生装置の構成図である。

DETAILED DESCRIPTION OF THE INVENTION

以下、本発明の実施の形態を、図面を参照して説明する。

（第１の実施形態）

図１は、本発明の第１の実施形態に係る暗号化・復号化システム全体を説明するブロック図である。サーバ１１とユーザ端末１２がネットワークを介して接続されている。ネットワークは、コンテンツデータの供給者が管理し、契約ユーザのみ使用できるものであってもよいし、インターネットのような誰でも使用できるものであってもよい。

図２は、同実施形態において使用されるユーザ端末１２の構成図である。ユーザ端末１２は、ＣＰＵ２１、メモリ２２、入力装置２３、ネットワークＩ／Ｆ（インターフェース）２４、出力装置２５、周辺装置Ｉ／Ｆ（インターフェース）２６と、復号化部２８から構成されている。

メモリ２２は、フラッシュメモリカードやハードディスクドライブ、ＲＯＭ、ＲＡＭ等である。入力装置２３は、キーボード、マウス等である。ネットワークＩ／Ｆ２４は、ネットワーク等ユーザ端末１２の外部の通信路に接続される。出力装置２５は、ディスプレイ等である。周辺装置Ｉ／Ｆ２６には、Ｈ／Ｗキー２７が差し込まれている。Ｈ／Ｗキー２７は、ユーザ端末１２の不正使用を防止するためのものである。ユーザ端末１２に正規のユーザのＨ／Ｗキー２７を差し込まないと、ユーザ端末１２は動作しない。復号化部２８は、後述するように、第１キーの復号化や、暗号化されたコンテンツデータの復号化を行う。

図３は、同実施形態における暗号化・復号化の動作を示すフローチャートである。前提として、ユーザは、情報提供者との間で事前に契約を締結し、ユーザＩＤ、パスワード、及びユーザ端末を動作させるためのＨ／Ｗキーを受領しているものとする。また、情報提供者は、各ユーザのユーザＩＤ、パスワード、とＨ／

Wキー情報をサーバに保管しているものとする。

ステップU１－１において、ユーザ端末１２のプログラムが起動される。ステップU１－２において、H／Wキー２７がユーザ端末１２の周辺装置I／F２６に差し込まれていることが確認されると、ステップU１－３において、サーバ１１への接続が要求される。サーバ１１は、ステップS１－１において、ユーザ端末１２からの接続要求を常時待っている。接続要求がユーザ端末１２からあれば、サーバ１１は、ステップS１－２において、ユーザ端末１２に対して、認証を促す。サーバ１１から認証を求められたユーザは、ステップU１－４において、ユーザ端末１１にユーザＩＤとパスワードを入力し、サーバ１１に送信する。サーバ１１は、ステップS１－３において、ユーザ情報データベースから、このユーザのユーザＩＤ、パスワード、H／WキーＩＤ等を検索する。サーバ１１は、ステップS１－４において、前記検索したユーザＩＤとパスワードが、ユーザ端末１２から受信したユーザＩＤとパスワードと一致するか否かを確認する。ユーザＩＤとパスワードが一致すれば、ステップS１－５において、配信コンテンツのリストなどの案内をユーザ端末１２に送信する。ユーザは、ステップU１－５において、配信を希望するコンテンツを指定し、ユーザ端末１２は、コンテンツ指定データと共に、可変パラメータをサーバ１１に送信する。また、ユーザ端末１１は、ステップU１－６において、前記可変パラメータを記憶する。

可変パラメータとは、コンテンツデータの配信回数、前回の通信時間、前回の通信日時、接続回数等、ユーザ端末１１毎に、毎回異なるパラメータをいう。

サーバ１１は、ステップS１－６において、ユーザ端末１２から送信されたコンテンツ指定データに基づいて、コンテンツデータベースからコンテンツ本体及びコンテンツ情報を検索する。

コンテンツ情報とは、各コンテンツを特定する情報であり、例えばコンテンツのサイズやコンテンツの前回更新日時等である。

サーバ１１は、S１－７において、検索したコンテンツ情報から第１キーを生成する。次に、ステップS１－８において、サーバ１１は、ユーザ端末１２から受信した可変パラメータと、ユーザ情報データベースから検索したそのユーザのH／WキーＩＤと、前記生成した第１キーとから、第２キーを生成し、ユーザ端

末１２に送信する。

ユーザ端末１２は、ステップＵ１－７において、可変パラメータを読み出す。ユーザ端末１２は、ステップＵ１－８において、第２キーをサーバ１１から受信し、読み出した可変パラメータと、第２キーと、Ｈ／Ｗキー ＩＤとから、第１キーを復号化する。

サーバ１１は、ステップＳ１－９において、配信するコンテンツ本体を第１キーで暗号化し、ユーザ端末１２に送信する。

ユーザ端末１２は、ステップＵ１－９において、サーバ１１から受信した暗号化されたコンテンツデータ本体を、先に復号化しておいた第１キーを用いて復号化する。

尚、上記動作の順序は、上記実施例の順序に限定されるものではない。サーバ１１とユーザ端末１２間でのコンテンツデータの配信及び暗号化・復号化に支障がない限り順序が変ってもよい。例えば、ステップＳ１－９がステップＳ１－７に続いて行なわれてもよい。

上記のようにサーバ１１にて生成される第２キーは、固定された生成要素だけでなく、毎回異なる可変パラメータを生成要素としている。これにより、ハッカー等の外部からの不正侵入による復号化キーの盗難や、その結果生じるコンテンツデータの不正な再生を防止することができる。

また、ユーザ端末１２に、サーバ１１から受信したコンテンツデータを保存できない機能を付加してもよい。これにより、ユーザは配信されたコンテンツデータを１回しか再生できず、再生による閲覧・視聴回数に応じた課金ができる。

（第２の実施例）

図４は、本発明の第２の実施形態における暗号化・復号化の動作を示すフローチャートである。前述した第１の実施形態と同一の動作部分については詳細な説明は省略する。

ユーザがユーザ端末１２のプログラムを起動させるステップＵ２－１から、サーバ１１が配信するコンテンツのリストなどの案内をユーザ端末１２に送信するステップＳ２－５までは、第１の実施形態と動作は同じである。

第２の実施形態が、第１の実施形態と異なるのは、ステップＵ２－５において、ユーザがコンテンツを指定し、ユーザ端末１２からサーバ１１に送信する際に、可変パラメータを併せて送信しない点である。そして、ユーザ端末１２にて、ステップＵ２－７において、コンテンツデータを復号化した後、ステップＵ２－８／ステップＳ２－１０において、ユーザ端末１２とサーバ１１間で、可変パラメータを同期処理する点である。

このようにすることで、一連のコンテンツの配信動作において、第２キーの生成要素の１つである可変パラメータを、ユーザ端末１２からサーバ１１に送信しないので、さらにセキュリティが高まる。

また、前記同期処理は、コンテンツデータ配信のための接続機会とは異なる接続機会において、実施してもよい。

Additional advantages and modifications will readily occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details and representative embodiments shown and described herein. Accordingly, various modifications may be made without departing from the spirit or scope of the general inventive concept as defined by the appended claims and their equivalents.

CLAIMS

1．ネットワークを介してサーバからユーザ端末に配信されるコンテンツデータの暗号化・復号化方法 comprising：

配信されるコンテンツデータのコンテンツ情報から、第１キーをサーバにて生成し、

可変パラメータと、Ｈ／ＷキーＩＤと、前記第１キーとから、第２キーをサーバにて生成し、生成された第２キーをユーザ端末に送信し、

可変パラメータと、Ｈ／ＷキーＩＤと、前記第２キーとから、第１キーをユーザ端末にて復号化し、

配信されるコンテンツデータを、前記第１キーで、サーバにて暗号化し、暗号化されたコンテンツデータをユーザ端末に送信し、and

暗号化されたコンテンツデータを、前記復号化された第１キーで、ユーザ端末にて復号化する。

2．コンテンツデータの暗号化・復号化方法 according to claim 1, the method further comprising:

ユーザ端末にて可変パラメータを生成し、生成された可変パラメータをサーバに送信する。

3．コンテンツデータの暗号化・復号化方法 according to claim 2， wherein 第２キーをサーバで生成するときに使用される可変パラメータは、ユーザ端末から送信された可変パラメータである。

4．コンテンツデータの暗号化・復号化方法 according to claim 1, the method further comprising:

ユーザ端末とサーバとの間で、可変パラメータを同期する。

5．コンテンツデータの暗号化・復号化方法 according to claim 4, wherein

前記同期は、コンテンツデータの配信とは異なるときに、ユーザ端末と

サーバとの間で実施する。

６．コンテンツデータの暗号化・復号化システム comprising：

a server、

the server comprising；

配信されるコンテンツデータのコンテンツ情報から、第１キーを生成する手段、

可変パラメータと、Ｈ／Ｗキー ＩＤと、前記第１キーとから、第２キーを生成する手段、and

配信されるコンテンツデータを第１キーで暗号化する手段、

a user terminal、

the user terminal comprising；

前記第２キーと前記暗号化されたコンテンツデータとを、前記サーバから受信するように構成されたネットワークインターフェース、

可変パラメータと、Ｈ／Ｗキー ＩＤと、前記第２キーとから、第１キーを復号化する手段、and

前記復号化された第１キーで、前記暗号化されたコンテンツデータを復号化する手段。

７．コンテンツデータの暗号化・復号化システム according to claim ６, the system further comprising:

前記サーバと、前記ユーザ端末との間で、可変パラメータを同期する手段。

８．ネットワークを介してサーバから配信されるコンテンツデータの暗号化・復号化に用いられる ユーザ端末 comprising：

配信されるコンテンツデータのコンテンツ情報から生成された第１キーと可変パラメータとＨ／Ｗキー ＩＤとから生成された第２キーと、前記第１キー

で暗号化されたコンテンツデータとを、サーバから受信するように構成されたネットワークインターフェース、and

可変パラメータとH／WキーＩＤと前記第２キーとから、第１キーを復号化し、復号化された第１キーで前記暗号化されたコンテンツデータを復号化するように構成された復号化部。

９．コンテンツデータの暗号化・復号化に用いられるユーザ端末 according to claim ５，ユーザ端末 further comprising:

サーバとの間で、可変パラメータを同期する手段。

ABSTRACT OF THE DISCLOSURE

配信されるコンテンツデータのコンテンツ情報から、第１キーをサーバにて生成する。可変パラメータと、Ｈ／ＷキーＩＤと、第１キーとから、第２キーをサーバにて生成し、生成された第２キーをユーザ端末に送信する。可変パラメータと、Ｈ／ＷキーＩＤと、第２キーとから、第１キーをユーザ端末にて復号化する。配信されるコンテンツデータを、第１キーで、サーバにて暗号化し、暗号化されたコンテンツデータをユーザ端末に送信する。暗号化されたコンテンツデータを、復号化された第１キーで、ユーザ端末にて復号化する。